UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/707,408	12/11/2003	David L. Kaminsky	014682.000002	1407

44870 7590 06/10/2009

MOORE & VAN ALLEN, PLLC For IBM
P.O. Box 13706
Research Triangle Park, NC 27709

EXAMINER	
MADAMBA, GLENFORD J	

ART UNIT	PAPER NUMBER
2451	

MAIL DATE	DELIVERY MODE
06/10/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/707,408
Filing Date: December 11, 2003
Appellant(s): David Kaminsky, Christina Cruz, Carrie Searcey, Eric Kirchstein

Frederick D. Bailey (42,282)
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed May 13, 2009 appealing from the Office action mailed December 29, 2008.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

7,032,022	SHANUMGAM	04-2006
6,981,029	MENDITTO	12-2005
6,621,793	WIDEGREN	09-2003
6,510,513	DANIELI	01-2003
2003/0110192	VALENTE	06-2003

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

1. Claims 1- 3, 10-15, 23-25, 27-29, 31, 35-38, and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shanumgam et al (hereinafter Shanumgam), U.S. Patent US 7,032,022 B1 in view of Menditto et al (hereinafter Menditto), U.S. Patent 6,981,029 and in further view of Applicant's Admitted own Prior Art (AAPA).

As per Claims 1, 11, 12, 23, 24 and 36, Shanumgam in view of Menditto discloses a method to distribute policies, comprising [Abstract]:

determining if a policy template is present at an enforcement point (Policy Enforcers 142 / 126) [Fig. 1] [col 1, L65 – col 2, L26] in response to receiving an

identification (ID) (i.e., Policy Identifier {ID}) [col 10, L53] assigned to the policy template at the enforcement point; (Menditto: [col 3, L1-29] [col 6, L16-53] [col 9, L37-62] [col 12, L20 –col 13, L6]) wherein the policy template includes a form of "if a first parameter then a second parameter", the policy template and the parameters being transmitted separately to reduce use of communication resources by factoring the template and parameters to be used in the template and to permit different parameters to be transmitted from time to time to replace previous parameters in the policy template without the need of transmitting the entire policy template again to further reduce use of communication resources;

transmitting a query from the enforcement point to a repository, where policy templates are stored, in response to the policy template not being present at the enforcement point, wherein the query includes the ID assigned to the policy template; (Menditto: [col 3, L1-29] [col 6, L16-53] [col 9, L37-62] [col 12, L20 –col 13, L6])

receiving the policy template at the enforcement point, wherein the policy template is transmitted by the repository in response to the query; (Menditto: [col 3, L1-29] [col 6, L16-53] [col 9, L37-62] [col 12, L20 –col 13, L6])and

receiving a set of parameters (i.e., attributes) [col 19, L49-65] to be used in the policy template (e.g., selected policy enforcer 'settings') [Abstract] [Fig. 5] [col 8,L20-54] at the enforcement point (i.e., 411) [Fig. 5] [Figs. 1-4, 13-14 & 17] [col 1, L65 – col 2, L26] wherein the set of parameters are transmitted separately from the policy template.

While Shanumgam discloses substantial features of the invention, such as Policy Server Database 130, Policy Enforcement Points 124 / 126, Policy Settings for the Policy Enforcers, and Policy Identifer (ID) Attribute 724 for identifying a particular policy rule in the list of policies, and a method of distributing / replicating the 'policies' (including their Policy ID) from Policy Server to Policy Enforcers 124 / 126, the additionally recited features of the method comprising the steps of determining if a policy template is present at an enforcement point in response to receiving an identification (ID) assigned to the policy template at the enforcement point; transmitting a query from the enforcement point to a repository, where policy templates are stored, in response to the policy template not being present at the enforcement point, wherein the query includes the ID assigned to the policy template; and receiving the policy template at the enforcement point, wherein the policy template is transmitted by the repository in response to the query are disclosed by Menditto in a related endeavor.

Menditto discloses as his invention an information service provider network that includes a content gateway to process requests for information from a client terminal. The content gateway includes a router for receiving a request for information from the client terminal. The router forwards the request according to the domain name to a selected one of a plurality of processors to further process the request. The selected one of the plurality of processors identifies an information source to satisfy the request in response to the additional content of the request [Abstract] [col 1, L45-53] [Figs. 1 & 3]. As part of his invention, Menditto discloses that "Content Gateways 18 distribute information from content providers 14 either directly or through content delivery nodes

22 to client terminals 16 according to Content Gateway Policy Manager 26 (CGPM). CGPM 26 is a management node in information service provider 12 that serves as a *repository* for *content policies* and communicates with content gateways 18 to distribute content policies within information service provider 12 and exchange policies with other CGPMs in other information service providers" [col 2, L43-53].

In particular, Menditto discloses the additionally recited features of the method comprising the steps of determining if a policy template is present at an enforcement point in response to receiving an identification (ID) assigned to the policy template at the enforcement point; transmitting a query from the enforcement point to a repository, where policy templates are stored, in response to the policy template not being present at the enforcement point, wherein the query includes the ID assigned to the policy template; and receiving the policy template at the enforcement point, wherein the policy template is transmitted by the repository in response to the query [col 3, L1-29][col 6, L16-53] (e.g., "...content policy may be *downloaded* to content gateway 18 *on-demand*...") [col 7, L1-53] [col 8, L27-30] (e.g., ...content policy associated with a query...receiving policy updates from CGPM 26 and processing subsequent requests according to the newly installed policy.) [col 9, L37-62] [col 12, L20 –col 13, L6].

It would thus be obvious to one of ordinary skill in the art at the time of the invention to combine and/or modify Shanumgam's invention with the above said additionally recited features, as disclosed by Menditto for the motivation of providing systems and method for processing a request for information in a network that has considerable advantages over conventional routing techniques (e.g. determining a

source of information based on the additional content of a request apart from the domain name associated therewith) [col 1, L54 – col 2, L2].

Further, while the combination of Shanumgam and Menditto discloses substantial features of the invention, as above, the additional recited feature of wherein the policy template includes a form of "if a first parameter then a second parameter", the policy template and the parameters being transmitted separately to reduce use of communication resources by factoring the template and parameters to be used in the template and to permit different parameters to be transmitted from time to time to replace previous parameters in the policy template without the need of transmitting the entire policy template again to further reduce use of communication resources is well-known and expressly disclosed in view of Applicant's Admitted own Prior Art.

With respect to Applicant's background for his own invention, Applicant states the following:

"Policies may be defined or developed to control software applications, network management, e-commerce or business or similar communications or data processing activities. Such policies may include 'if-then' clauses or similar statements or definitions. An example of one policy may be "if some precondition, then perform some predefined action, or set some value or the like." In another example, the policy may be "if some precondition and some other precondition or preconditions, then perform some predefined action, set some value or the like." Policies can have a typical lifecycle.

Over time, policies may be updated to meet changing conditions or needs or may become outdated and deleted or changed to new policies. Efficiently defining, storing, distributing and enforcing policies can be a challenge. Under some circumstances only minor changes or selected parameters or values used in a policy or related group of policies may need to be changed. Defining an entirely new policy or policies, distributing the policies to all enforcement points and making adjustments at each of the enforcement points to implement and enforce the policies may be burdensome, time consuming and involve inefficient use of limited data processing, storage and communication resources." [Application Background of the Invention: 0002]

It would thus be obvious to combine and/or modify the combination of Shanumgam and Menditto with the above well-known feature as disclosed by Applicant for the motivation of efficiently providing 'updates' to policies and/or policy templates that defined the policies, including policy parameters that comprise the policy / policy templates.

Claims 11, 12, 23, 24 and 36 recite the same limitations as claim 1, are distinguished only by statutory category, and thus rejected on the same basis.

As per Claims 2, 13, 29 and 37, Shanumgam discloses the method of claim 1, binding the parameters to the policy template [Abstract] [Figs. 5 & 17] [col 20, L22-47].

As per Claims 3, 14 and 38, Shanumgam discloses the method of claim 2, further comprising implementing the policy associated with the policy template [Figs. 1-5, 15 & 17] [col 1, L65 – col 2, L26].

As per Claim 15, Shanumgam discloses the method of claim 11, further comprising storing each one of the at least one set of parameters by name and type [col 13, L24-30].

As per Claims 31 and 40, Shanumgam discloses the method of claim 1, further comprising transmitting any policy templates to the enforcement point or any of the selected enforcement points in response to a query from the enforcement point or any of the selected enforcement points including any IDs assigned to the policy templates.

As per Claims 10, 28 and 35, Shanumgam in view of Menditto discloses a method to distribute policies, comprising:

defining a policy template associated with each policy; assigning a unique identification (ID) to each policy template [Abstract]; wherein the policy template includes a form of "if a first parameter then a second parameter", the policy template and the parameters being transmitted separately to reduce use of communication resources by factoring the template and parameters to be used in the template and to permit different parameters to be transmitted from time to time to replace previous

parameters in the policy template without the need of transmitting the entire policy template again to further reduce use of communication resources;

storing each policy template and assigned ID (130) [Fig. 1]; and

transmitting only the assigned ID to an enforcement point for each policy to be enforced by the enforcement point, wherein only the ID is transmitted to the enforcement point rather than the policy template to substantially minimize use of data processing and communication resources (i.e., 411) [Fig. 5] [Figs. 1-4, 13-14 & 17] [col 1, L65 – col 2, L26];

determining if a policy template is present at an enforcement point (Policy Enforcers 142 / 126) [Fig. 1] [col 1, L65 – col 2, L26] in response to receiving an identification (ID) (i.e., Policy Identifier {ID}) [col 10, L53] assigned to the policy template at the enforcement point; (Menditto: [col 3, L1-29] [col 6, L16-53] [col 9, L37-62] [col 12, L20 –col 13, L6])

transmitting a query from the enforcement point to a repository, where policy templates are stored, in response to the policy template not being present at the enforcement point, wherein the query includes the ID assigned to the policy template; (Menditto: [col 3, L1-29] [col 6, L16-53] [col 9, L37-62] [col 12, L20 –col 13, L6])

receiving the policy template at the enforcement point, wherein the policy template is transmitted by the repository in response to the query; (Menditto: [col 3, L1-29] [col 6, L16-53] [col 9, L37-62] [col 12, L20 –col 13, L6]) and

receiving a set of parameters (i.e., attributes) [col 19, L49-65] to be used in the policy template (e.g., selected policy enforcer 'settings') [Abstract] [Fig. 5] [col 8,L20-54] at the enforcement point (i.e., 411) [Fig. 5] [Figs. 1-4, 13-14 & 17] [col 1, L65 – col 2, L26].

While Shanumgam discloses substantial features of the invention, such as Policy Server Database 130, Policy Enforcement Points 124 / 126, Policy Settings for the Policy Enforcers, and Policy Identifer (ID) Attribute 724 for identifying a particular policy rule in the list of policies, and a method of distributing / replicating the 'policies' (including their Policy ID) from Policy Server to Policy Enforcers 124 / 126, the additionally recited features of the method comprising the steps of determining if a policy template is present at an enforcement point in response to receiving an identification (ID) assigned to the policy template at the enforcement point; transmitting a query from the enforcement point to a repository, where policy templates are stored, in response to the policy template not being present at the enforcement point, wherein the query includes the ID assigned to the policy template; and receiving the policy template at the enforcement point, wherein the policy template is transmitted by the repository in response to the query are disclosed by Menditto in a related endeavor.

Menditto discloses as his invention an information service provider network that includes a content gateway to process requests for information from a client terminal. The content gateway includes a router for receiving a request for information from the client terminal. The router forwards the request according to the domain name to a

selected one of a plurality of processors to further process the request. The selected one of the plurality of processors identifies an information source to satisfy the request in response to the additional content of the request [Abstract] [col 1, L45-53] [Figs. 1 & 3]. As part of his invention, Menditto discloses that "Content Gateways 18 distribute information from content providers 14 either directly or through content delivery nodes 22 to client terminals 16 according to Content Gateway Policy Manager 26 (CGPM). CGPM 26 is a management node in information service provider 12 that serves as a *repository* for *content policies* and communicates with content gateways 18 to distribute content policies within information service provider 12 and exchange policies with other CGPMs in other information service providers" [col 2, L43-53].

In particular, Menditto discloses the additionally recited features of the method comprising the steps of determining if a policy template is present at an enforcement point in response to receiving an identification (ID) assigned to the policy template at the enforcement point; transmitting a query from the enforcement point to a repository, where policy templates are stored, in response to the policy template not being present at the enforcement point, wherein the query includes the ID assigned to the policy template; and receiving the policy template at the enforcement point, wherein the policy template is transmitted by the repository in response to the query [col 3, L1-29][col 6, L16-53] (e.g., "...content policy may be *downloaded* to content gateway 18 *on-demand*...") [col 7, L1-53] [col 8, L27-30] (e.g., ...content policy associated with a query...receiving policy updates from CGPM 26 and processing subsequent requests according to the newly installed policy.) [col 9, L37-62] [col 12, L20 –col 13, L6].

It would thus be obvious to one of ordinary skill in the art at the time of the invention to combine and/or modify Shanumgam's invention with the above said additionally recited features, as disclosed by Menditto for the motivation of providing systems and method for processing a request for information in a network that has considerable advantages over conventional routing techniques (e.g. determining a source of information based on the additional content of a request apart from the domain name associated therewith) [col 1, L54 – col 2, L2].

Further, while the combination of Shanumgam and Menditto discloses substantial features of the invention, as above, the additional recited feature of wherein the policy template includes a form of "if a first parameter then a second parameter", the policy template and the parameters being transmitted separately to reduce use of communication resources by factoring the template and parameters to be used in the template and to permit different parameters to be transmitted from time to time to replace previous parameters in the policy template without the need of transmitting the entire policy template again to further reduce use of communication resources is well-known and expressly disclosed in view of Applicant's Admitted own Prior Art.

With respect to Applicant's background for his own invention, Applicant states the following:

"Policies may be defined or developed to control software applications, network management, e-commerce or business or similar communications or data processing

activities. Such policies may include 'if-then' clauses or similar statements or definitions. An example of one policy may be "if some precondition, then perform some predefined action, or set some value or the like." In another example, the policy may be "if some precondition and some other precondition or preconditions, then perform some predefined action, set some value or the like." Policies can have a typical lifecycle. Over time, policies may be updated to meet changing conditions or needs or may become outdated and deleted or changed to new policies. Efficiently defining, storing, distributing and enforcing policies can be a challenge. Under some circumstances only minor changes or selected parameters or values used in a policy or related group of policies may need to be changed. Defining an entirely new policy or policies, distributing the policies to all enforcement points and making adjustments at each of the enforcement points to implement and enforce the policies may be burdensome, time consuming and involve inefficient use of limited data processing, storage and communication resources." [Application Background of the Invention: 0002]

It would thus be obvious to combine and/or modify the combination of Shanumgam and Menditto with the above well-known feature as disclosed by Applicant for the motivation of efficiently providing 'updates' to policies and/or policy templates that defined the policies, including policy parameters that comprise the policy / policy templates.

As per Claim 25, Shanumgam discloses the system of claim 23, wherein each enforcement point comprises:

a processor to receive the IDs assigned to each policy template (policy server 122 / policy enforcers 124 / 126) [Fig. 1]; and

a data source to store each policy template for enforcement and assigned ID, wherein the processor forms and transmits a query in response to each policy template corresponding to any transmitted IDs not present in the data source (e.g., repositories 130, 132, 134) [Fig. 1] [Figs. 3-4 & 12-19]

As per Claim 27, Shanumgam discloses the system of claim 26, further comprising a server to interface between each policy administrator, each enforcement point and the repository [Fig. 1].

2. Claims 6, 18, 32 and 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shanumgam et al (hereinafter Shanumgam), U.S. Patent US 7,032,022 B1 in view of Menditto et al (hereinafter Menditto), U.S. Patent 6,981,029 and in further view of Widegren et al (hereinafter Widegren), U.S. Patent 6,621,793.

As per Claims 6, 18, 32 and 41, Shanumgam in view of Menditto and in further view of Widegren discloses the method of claim 1, further comprising applying asynchronous, out-of-band communication to transmit the query and any policy templates.

While the combination of Shanumgam and Menditto discloses substantial features of the invention such as the method of claim 5, and transmitting of policy templates in response to a query from the enforcement points, the added feature of the method further comprising applying asynchronous, out-of-band communication to transmit the query and any policy templates is disclosed by Widegren in a related endeavor.

Widegren discloses as his invention a method of filtering and gating data flow in a QoS connection between a remote host and user equipment in a packet data network using policy control mechanisms includes a remote host initiating an application in an application server and a corresponding session between the remote host and the user equipment ("UE") via the application server. The UE requests, to a gateway support node ("GGSN") of the network, establishment of a network bearer service between the UE and the remote host. A corresponding policy control function ("PCF") in a policy server receives, from the application server, filtering data derived from session data received by the application server during the session. The GGSN interrogates the corresponding PCF in the policy server to initialize a gate using policy control filtering data at the GGSN. The gate then filters the data flow in the QoS connection according to the policy control filtering data [Abstract]. In particular,

Widegren discloses the added feature of the method further comprising applying asynchronous, out-of-band communication to transmit the query and any policy templates (e.g., asynchronous notification) [col 22, L41-53].

It would thus be obvious to one of ordinary skill in the art at the time of the invention to modify the combination of Shanumgam and Menditto's invention with the added feature of the method further comprising applying asynchronous, out-of-band communication to transmit the query and any policy templates, as disclosed by Widegren, for the motivation of providing a method of filtering and gating data in packet data networks using policy mechanisms [col 1, L15-17].

3. Claims 7, 19, 20, 33 and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shanumgam et al (hereinafter Shanumgam), U.S. Patent US 7,032,022 B1 in view of Menditto et al (hereinafter Menditto), U.S. Patent 6,981,029 and in further view of and in further view of Danieli, U.S. Patent 6,510,513.

As per Claims 7, 19, 20, 33 and 42, Shanumgam view of Menditto and in further view of Danieli discloses the method of claim 1, further comprising compressing each policy template before transmitting to the enforcement point or any of the selected enforcement points.

While the combination of Shanumgam and Menditto discloses substantial features of the invention such as the method of claim 5, and transmitting of policy templates in response to a query from the enforcement points, the added feature of the method further comprising compressing each policy template before transmitting to the enforcement point or any of the selected enforcement points is disclosed by Danieli in a related endeavor.

Danieli discloses as his invention a Security services and policy enforcement for electronic data. A first client generates a digest from the electronic data, and submits a security certificate request containing the digest to a trusted arbitrator server, where the request is time stamped and logged. The trusted arbitrator authenticates the first client's credentials and returns the security certificate to the first client. The data and security certificate are combined to create a distribution unit. A second client acquires the distribution unit, extracts the security certificate, and generates a digest from the data. If the digest from the second client matches the logged digest from the first client, the data is valid. Depending on the certificate type and policy level, the trusted arbitrator server provides other services to the clients, such as notification of improper user of the data [Abstract]. In particular, Danieli discloses the added feature of the method further comprising compressing each policy template before transmitting to the enforcement point or any of the selected enforcement points [col 16, L21-36].

It would thus be obvious to one of ordinary skill in the art at the time of the invention to modify the combination of Shanumgam and Menditto's invention with the added feature of the method further comprising compressing each policy template

before transmitting to the enforcement point or any of the selected enforcement points, as disclosed by Danieli, for the motivation of providing a system and method for authenticating and validating electronic data and enforcing restrictions (e.g. policies) on the use of electronic data [col 1, L5-10].

4. Claims 8, 9, 21, 22, 34, 43 and 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shanumgam et al (hereinafter Shanumgam), U.S. Patent US 7,032,022 B1 in view of Menditto et al (hereinafter Menditto), U.S. Patent 6,981,029 and in further view of Valente et al (hereinafter Valente), U.S. Patent Publication US 2003/0110192 A1.

As per Claims 8, 21, 34 and 43, Shanumgam in view of Menditto and in further view of Valente discloses the method of claim 1, further comprising forming the policy template in a structured document.

While the combination of Shanumgam and Menditto discloses substantial features of the invention such as the method of claim 1, and transmitting of policy templates in response to a query from the enforcement points, the added feature of the method further comprising forming each policy template in a structured document (e.g., XML document) is disclosed by Valente in a related endeavor.

Valente discloses as his invention a Security services and policy enforcement for electronic data. A first client generates a digest from the electronic data, and submits a

security certificate request containing the digest to a trusted arbitrator server, where the request is time stamped and logged. The trusted arbitrator authenticates the first client's credentials and returns the security certificate to the first client. The data and security certificate are combined to create a distribution unit. A second client acquires the distribution unit, extracts the security certificate, and generates a digest from the data. If the digest from the second client matches the logged digest from the first client, the data is valid. Depending on the certificate type and policy level, the trusted arbitrator server provides other services to the clients, such as notification of improper user of the data [Abstract]. In particular, Valente discloses the added feature of the method further comprising forming each policy template in a structured document [Abstract] (e.g., XML file 602a) [Fig. 6].

It would thus be obvious to one of ordinary skill in the art at the time of the invention to modify the combination of Shanumgam and Menditto's invention with the added feature of the method further comprising forming each policy template in a structured document (e.g., XML document), as disclosed by Valente, for the motivation of providing a system and method for authenticating and validating electronic data and enforcing restrictions (e.g. policies) on the use of electronic data [col 1, L5-10].

As per Claims 9, 22 and 44, Shanumgam in view of Menditto and in further view of Valente disclosthe method of claim 1, further comprising forming the policy template in a mark-up language.

While the combination of Shanumgam and Menditto discloses substantial features of the invention such as the method of claim 5, and transmitting of policy templates in response to a query from the enforcement points, the added feature of the method further comprising forming each policy template in a mark-up language is disclosed by Valente in a related endeavor.

Valente discloses as his invention a Security services and policy enforcement for electronic data. A first client generates a digest from the electronic data, and submits a security certificate request containing the digest to a trusted arbitrator server, where the request is time stamped and logged. The trusted arbitrator authenticates the first client's credentials and returns the security certificate to the first client. The data and security certificate are combined to create a distribution unit. A second client acquires the distribution unit, extracts the security certificate, and generates a digest from the data. If the digest from the second client matches the logged digest from the first client, the data is valid. Depending on the certificate type and policy level, the trusted arbitrator server provides other services to the clients, such as notification of improper user of the data [Abstract]. In particular, Valente discloses the added feature of the method further comprising forming each policy template in a mark-up language [Abstract] (e.g., XML file 602a) [Fig. 6].

It would thus be obvious to one of ordinary skill in the art at the time of the invention to modify the combination of Shanumgam and Menditto's invention with the added feature of the method further comprising forming each policy template in a structured document (e.g., XML document), as disclosed by Valente, for the motivation

of providing a system and method for authenticating and validating electronic data and enforcing restrictions (e.g. policies) on the use of electronic data [col 1, L5-10].

(10) Response to Argument

Claims 1-3, 10-15, 23-25, 27-29, 31, 35-38 and 40

With respect to claims 1, 10, 23, 28 and 35, and claim 1 in particular, Applicant firstly argues that none of the cited references, either alone or in combination, teach or disclose particular feature(s) of the claim, which recites in part: "determining if a policy template is present at an enforcement point in response to receiving an identification assigned to the policy template. The Office respectfully disagrees and submits that Applicant has misinterpreted and/or not fully considered all of the teachings and disclosures of the applied prior art reference(s).

In support of his argument, Applicant remarks that the citations to Shanumgam merely disclose a system that includes a *central policy server* defining policy settings for edge devices ('*policy enforcers*') associated with networks, and monitoring the health and status of the *policy enforcers* from a single location, wherein the edge devices perform the role of 'policy enforcers' for their respective networks and manage policies for their network according to their stored policy settings. Applicant also remarks that

although Shanumgam additionally teaches and discloses 'policies', such as a firewall policy, including a *policy identifier attribute* for identifying a particular policy rule in the list of policies, Applicant contends that this is not the same as "determining if a policy template is present at an enforcement point in response to receiving an identification assigned to a policy template", as recited by the claims. Applicant further remarks that Shanumgam merely discloses that a policy includes a *policy identifier* and that a central policy server monitors policy enforcers that each have resources for managing policies of the network; and thus does not disclose or suggest "a policy *template* beinq present at an enforcement point", nor "receivinq an 'identification' assigned to the policy template to determine if the policy template is present". The Office respectfully disagrees.

In response to the argument, the Office remarks and asserts that the above argued features and deficiencies of Shanumgam are, in fact, disclosed and resolved by at least Menditto. For example, Menditto expressly discloses that "Content Gateway Policy Manager 26 is a 'management node'... that serves as a '*repository*' for content policies and communicates with Content Gateways 18 to 'distribute' content policies with information service provider 12 and exchange policies with other content gateway policy managers in other information service providers [col 2,L45-52]. Menditto additionally discloses that Content Gateway 18 participates in a policy distribution network to *receive* and install content policies and supports content peering in order to

direct requests to content gateways or content delivery nodes in other information service providers 12 [col 3, L21-25].

Further, in one embodiment, Menditto expressly teaches that

"Content gateway directory 32 codifies a *policy* for content based routing. Content gateway directory 32 includes a classification policy and a processing policy. The *classification policy* defines the pattern or '*template*' used to match the domain name and additional content of the request from client terminal 16." [col 6, L41-46].

Significantly, Menditto also teaches the following:

Since valid domain name table 34 is relatively small and is not designed to hold every possible domain name that has an associated content policy for execution by a content gateway processor 30, there may be a content policy for a domain name within content gateway policy manager 26. In parallel, the *domain name server query* is also forwarded to content gateway policy manager 26 along path D. Content gateway policy manager 26 '*determines*' if there is a content policy associated with the ***query***. Content gateway policy manager 26 searches its policy database for policy information. If no policy exists, then no action is taken. If a policy exists for the domain, the policy is provided to content gateway router 28 along path E.

[Menditto: col 9, L37-50]

Moreover, Menditto expressly discloses a 'Policy ID' for identifying a policy (Appendix A) [col 16] and a Classification Policy for defining '*templates*' (Appendix A)

[col 16] [col 6, L25-30] for the classification of URL requests. He also teaches that "a policy distribution point responsible for distributing policies to other network elements is connected to content gateway policy manager 26 and may send 'policy updates' to other content gateways 18 and content gateway managers 26 as appropriate [col 7, L9-13].

Given the above disclosures and features, it is thus clear that Menditto's invention expressly teaches a Policy Manager providing / distributing 'policies' and/or 'policy updates' to a content gateway router 28 or peer device (that does not yet have the particular policy or update in its policy database), in response to a *query*. It is also thus clear that the 'existing policy' or 'policy update' to be provided / distributed (e.g., Classification Policy that defines a 'template', or Processing Policy) can be identified using the 'Policy ID' feature of Menditto's invention. The argued feature of "determining if a policy template is present at an enforcement point in response to receiving an identification assigned to the policy template" is thus expressly taught by at least Menditto.

With regards to the argued feature, the Office secondly remarks and notes that, assuming any deficiencies in the disclosures of Menditto (which there are none), the argued feature of "determining if a policy template is present at an enforcement point in response to receiving an identification assigned to the policy template" is also obvious and well-known in the art. In this regard, the Office submits as 'supporting evidence'

related inventions to Lortz, (US Patent 6,957,261) and Bakshi el al. (US Patent 7,441,263), which alternatively teaches and discloses the argued feature of distributing and/or providing 'policy' / 'multi-policy templates' to devices that do not yet have the particular 'policy or 'policy template', and that are identified by a Policy identifier or ID. The supplementary prior art - cited but not referred to in the Final Office Action - was provided to Applicant as 'evidence' of well-known features and practices in the art with respect to the above argued features.

Significantly, Bakshi, for example, expressly discloses the well-known feature of one or more policy template(s) (i.e., "multi-template policy") wherein a 'policy' may be created and stored with user credentials as 'templates' in a database of his invention [col 14, L58 – 67] [col 16, L26 – col 17, L56] [Tables 1, 2 & 3]. With reference to Tables 2 and 3, for example, Bakshi expressly illustrates a *policy listing*, wherein each *policy* is identified by a unique *policy identifier* (i.e., Policy ID) and wherein the policy '*template*' is defined by 'attributes' such as a GUID (i.e., '1234-5678-9101') and/or Online Username (i.e., 'jsmith.user.tradeonline.com'). The features of a 'policy' or 'policy template' that can be uniquely identified by a Policy ID (and which can accordingly be stored, queried, and transmitted or distributed) are thus obvious and well-known in the art, and at the very least obviously applies to the disclosed inventions of Shanumgam and/or Menditto.

Lortz discloses as his invention Resource Policy Management using a Centralized Policy Data Structure. 'Managing policies' includes receiving policy data associated with a resource from a resource owner (user device) over a network, authenticating the resource owner to determine whether to accept the received policy data, and storing the received policy data in a centralized data structure if the resource owner is authenticated [Abstract] [Figs. 1 & 2]. Significantly, Lortz expressly discloses as well-known and obvious the features of a policy associated with a device (i.e., devicepolicy 22a) [Fig. 3a], a policy associated with a user (i.e., userpolicy 22b) [Fig. 3b], as well as the corresponding identifier uniquely identifying the device policy (i.e., policyidentifier = '123') [Fig. 3a]. Lortz also expressly discloses receiving "*policy queries"* from a resource owner (200) [Fig.4b], the policy query including a "policy identifier" for identifying the associated user or device policy; evaluating the policy query [col 5, L45 – col 6, L13], and searching, retrieving and providing the appropriate *policy data* in the centralized policy data structure 22 to the resource device 14 [col 6, L45-60]. The argued feature of "transmitting a *query* (policy query) from an enforcement point to a repository, where the policy templates are stored in response to the policy template not being present at the enforcement point, wherein the query includes the ID assignment (policy identifier) to the policy template", as recited by the claims, is thus obvious and well-known to one of ordinary skill in the art, and also obviously applies to the disclosed inventions of Shanumgam and/or Menditto at the very least.

Further, with respect to claims 1, 10, 23, 28 and 35, Applicant secondly argues that none of the cited references teach or disclose "the policy template and the parameters being transmitted separately". The Office respectfully disagrees.

In response to the argument, the Office reiterates that the above argued feature is expressly taught or disclosed in view of Applicant's own admitted prior art teachings. As noted in the previous Office action / rejection, the above argued feature is also well-known in the art and expressly disclosed in view of Applicant's Admitted own Prior Art.

With respect to Applicant's background for his own invention, Applicant expressly states the following:

> "Policies may be defined or developed to control software applications, network management, e-commerce or business or similar communications or data processing activities. Such policies may include 'if-then' clauses or similar statements or definitions. An example of one policy may be "if some precondition, then perform some predefined action, or set some value or the like." In another example, the policy may be "if some precondition and some other precondition or preconditions, then perform some predefined action, set some value or the like." Policies can have a typical lifecycle. Over time, policies may be updated to meet changing conditions or needs or may become outdated and deleted or changed to new policies. Efficiently defining, storing, '*distributing*' and enforcing policies can be a challenge. Under some circumstances *only* 'minor

changes' or 'selected parameters or values' used in a policy or related group of policies may need to be changed. Defining an 'entirely new policy or policies', *distributing* the policies to all enforcement points and making adjustments at each of the enforcement points to implement and enforce the policies may be burdensome, time consuming and involve *inefficient use* of limited data processing, storage and *communication resources*."

[Application Background of the Invention: 0002]

Based on the above disclosure, it is clear that in certain circumstances, "only the *minor changes* or *selected parameters / values* of a policy or related group of policies" need to be changed, stored and/or *distributed* (transmitted); rather than distributing / transmitting the "entire" new or updated policy (or policies) to all enforcement points. As acknowledged and expressly taught above by Applicant in the background for his invention, sending the entire new or updated 'policy' (policy template) is not desirable as it leads to "inefficient use of limited processing, storage and *communication resources* (such as 'transmission bandwidth'). As such, it is obvious to one of ordinary skill in the art that the policy template and the parameters should be transmitted separately, whenever possible, to optimize or make the most efficient use of limited network resources. The argued feature of "parameters transmitted separately from the policy template" is thus obvious and well-known in the art in view of the above disclosure by Applicant. Alternatively, at least Shanumgam expressly teaches that only 'changes' or 'updates' to policy and/or 'policy settings' made at the central policy server are

automatically transferred to the policy enforcers for updating their respective databases [Shanumgam: Abstract] [col 20, L22-47] [col 21, L5-10]. The argued feature is thus also taught or disclosed by Shanumgam.

Lastly, with regards to the claims, Applicant argues that none of the references disclose or suggest "transmitting a query from the enforcement point to a repository, where policy templates are stored, in response to the policy template not being present at the enforcement point, wherein the query includes the ID assigned to the policy template". However, it has been previously discussed above that at least Menditto teaches these features; further, it has also been established that the argued features of a 'policy', 'policy template', 'policy query', and associated 'policy identifier' are at the very least obvious and well-known in the art, and the Office thus maintains its rejection of the claims for at least these reasons.

Regarding dependent claims 2, 3, 11 - 15, 24, 25, 27, 29, 31, 36 -38 and 40, the Office notes that the claims are dependent on one of independent claims 1, 10, 23, 28, 35, and inherits all of the features of their respective parent claim. The rejection of the claims is accordingly maintained for at least the same reasons provided for the rejection of the independent claims.

Claims 6-9, 18-22, 32-34 and 41-44

Regarding dependent claims 6-9, 18-22, 32-34, and 4-44, the Office notes that these claims are also dependent on one of 1, 10, 28 and 35 and, therefore, are not patentable for at least their dependency on their respective parent claims and for the same reasons provided for the rejection of their respective parent independent claims.

Accordingly, since it has also been shown that all of the limitations of the argued claims are taught and/or disclosed by the combination of Shanumgam, and/or Menditto, the Office maintains its rejection of the claims in view of the applied prior art references and their respective disclosures and teachings.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

(12) Conclusion

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Glenford Madamba
June 4, 2009

/John Follansbee/
Supervisory Patent Examiner, Art Unit 2451

Conferees:

/Jeffrey Pwu/

Supervisory Patent Examiner, Art Unit 2446

/John Follansbee/
Supervisory Patent Examiner, Art Unit 2451

John Follansbee

Frederick D. Bailey
Moore & Van Allen PLLC
P.O.Box 13706
Research Triangle Park, NC 27709